

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2005-020105**

(43)Date of publication of application : **20.01.2005**

(51)Int.Cl.

H04L 9/32

H04L 9/08

(21)Application number : **2003-178693**

(71)Applicant : **TAKANO NAOTO**

(22)Date of filing : **23.06.2003**

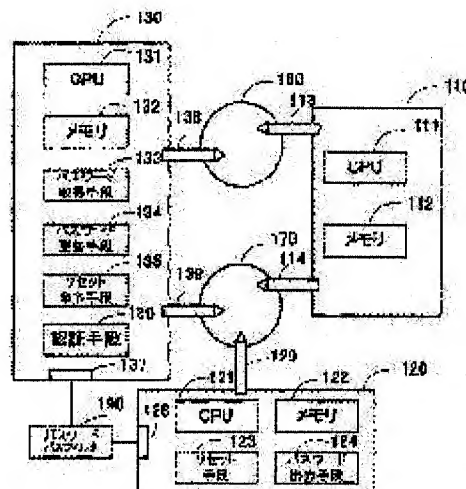
(72)Inventor : **TAKANO NAOTO**

## (54) COMMUNICATION UNIT, INFORMATION COMMUNICATION SYSTEM, AND INFORMATION COMMUNICATION METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To prevent leakage of data and falsification of data in a communication unit at a data transmission side or a communication unit at a data receiver side.

**SOLUTION:** The communication unit includes: an HD 170 for storing received encrypted data; an HD 160 for storing the transmitted encryption data; an information processing apparatus 110 for writing the received encrypted data in the HD 170 and for reading the encrypted data being a transmission object from the HD 160; an information processing apparatus 120 for reading the encrypted data stored in the HD 170 and decrypting the encrypted data by using a private key; an authentication means 130 for authenticating a password attached to the data decrypted by the information processing apparatus 120 and a password transmitted in advance; an information processing apparatus 130 for reading the encrypted data which are stored in the HD 170 and the password of which is confirmed for the coincidence with the password transmitted in advance by the authentication means 130, and writing the encrypted data being the transmission object to the HD 160; and a reset means 123 for resetting the encrypted data read by the information processing apparatus 120.



JP 2005-20105 A 2005.1.20

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-20105

(P2005-20105A)

(43) 公開日 平成17年1月20日(2005.1.20)

(51) Int.Cl.<sup>1</sup>

F1

テーマコード(参考)

H04L 9/32

H04L 9/00 673A

5J104

H04L 9/08

H04L 9/00 601A

審査請求 未請求 請求項の数 4 〇 L (全 14 頁)

(21) 出願番号 特願2003-178693 (P2003-178693)  
 (22) 出願日 平成15年6月23日(2003.6.23)

(71) 出願人 300023730  
 ▲高▼野 直人  
 千葉県千葉市花見川区堀町662番地の2  
 14  
 (74) 代理人 100092048  
 弁理士 沢田 雅男  
 (72) 発明者 高野 直人  
 千葉県花見川区堀町662-214  
 Fターム(参考) 5J104 AA07 KA01 NA05 PA07

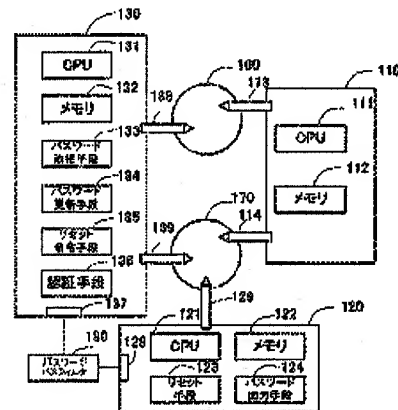
(54) 【発明の名称】 通信ユニット、情報通信システムおよび情報通信方法

(57) 【要約】

【課題】 データの漏洩、改ざんを防止する。

【解決手段】 受信した暗号化データを記憶するHD170と、送信する暗号化データを記憶するHD160と、受信した暗号化データをHD170に書き込むとともに送信対象の暗号化データをHD160から読み出す情報処理装置110と、HD170に記憶されている暗号化データを読み出して秘密キーを用いて暗号化データを復号化する情報処理装置120と、情報処理装置120によって復号化されたデータに付加されているパスワードとあらかじめ送ったパスワードとを認証する認証手段130と、認証手段130によってパスワード相互が一致したことが確認されたにHD170に記憶されている暗号化データを読み出すとともに送信対象の暗号化データをHD160に書き込む情報処理装置130と、情報処理装置120によって読み出した暗号化データをリセットするリセット手段123とを備える。

【選択図】 図2



(2)

JP 2005-20105 A 2005.1.20

## 【特許請求の範囲】

## 【請求項1】

データを送受信するのに先立って、ネットワーク接続されている他の通信ユニットとの間で、データを暗号化するための公開キーを交換するとともに、データの受信時には初回の当該データの受信前に前記他の通信ユニットに対して秘匿性が保持されるルートを通じて前記データに付加させるパスワードを送り、かつ当該他の通信ユニットに対して送信対象のデータに前記パスワードを付加してから自己の公開キーを用いて暗号化してなる暗号化データを作成するように促し、実際に当該他の通信ユニットから送信されてきた前記暗号化データを自己の公開キーに対応する秘密キーを用いて復号化を行い、

10

データの送信時には当該送信前に前記他の通信ユニットから秘匿性が保持されるルートを通じて送信されたパスワードを付加した送信対象のデータを当該他の通信ユニットの公開キーを用いて暗号化することによって作成した暗号化データを前記他の通信ユニットに対して送信する通信ユニットであって、

前記他の通信ユニットから送信された暗号化データを記憶する第1の記憶部と、

前記他の通信ユニットに送信する暗号化データを記憶する第2の記憶部と、

前記他の通信ユニットから送信された暗号化データを前記第1の記憶部に書き込むとともに前記他の通信ユニットに送信する暗号化データを前記第2の記憶部から読み出す第1の情報処理装置と、

前記第1の記憶部に記憶されている暗号化データを読み出して前記自己の秘密キーを用いて復号化する第2の情報処理装置と、

20

前記第2の情報処理装置によって復号化されたデータに付加されていたパスワードとあらかじめ前記他の通信ユニットに送ったパスワードとを認証する認証手段と、

前記認証手段によってパスワード相互の一致が確認されたときに前記第1の記憶部に記憶されている暗号化データを復号化したデータを取得するとともに前記他の通信ユニットへ送信する暗号化データを前記第2の記憶部に書き込む第3の情報処理装置とを備えることを特徴とする通信ユニット。

## 【請求項2】

前記認証手段は、ディスプレイ、プリンタ、スピーカ、前記パスワードをパスするフィルタのいずれかであることを特徴とする請求項1記載の通信ユニット。

30

## 【請求項3】

請求項1または2記載の通信ユニットを複数備え、当該通信ユニット相互をネットワークで接続してなる情報通信システム。

## 【請求項4】

データを送受信するのに先立って、ネットワーク接続されている通信ユニット間で、データを暗号化するための公開キーを交換するとともに、初回の当該データの送受信前にデータ送信先の通信ユニットからデータ送信元の通信ユニットに対して秘匿性が保持されるルートを通じて前記データに付加させるパスワードを送り、

前記データ送信元の通信ユニットで、前記パスワードを付加した送信対象のデータを前記データ送信先の通信ユニットの公開キーを用いて暗号化することによって作成した暗号化データを、前記データ送信先の通信ユニットに対して送信するとともに、

40

前記データ送信先の通信ユニットで、前記データ送信元の通信ユニットから送信されてきた暗号化データを自己の公開キーに対応する秘密キーを用いて復号化を行う情報通信方法であって、

前記データ送信元の通信ユニットは、

第1の情報処理装置によって、前記データ送信先の通信ユニットへ送信する暗号化データを第1の記憶部に書き込み、

前記ネットワークに直接接続している第2の情報処理装置によって、前記第1の記憶部に記憶してある暗号化データを読み出し、

前記データ送信先の通信ユニットは、

50

(3)

JP 2005-20105 A 2005.1.20

前記ネットワークに直接接続している第3の情報処理装置によって、前記データ送信元の通信ユニットから送信されてきた暗号化データを第2の記憶部に書き込み、  
第4の情報処理装置によって、前記第2の記憶部に記憶してある暗号化データの復号化を行い、  
前記第4の情報処理装置によって復号化されたデータに付加されていたパスワードとあらかじめ送っているパスワードとが一致した場合に、第5の情報処理装置によって、前記第2の記憶部に記憶されている暗号化データを復号化したデータを取得することを特徴とする情報通信方法。

【発明の詳細な説明】

【0001】

10

【発明が属する技術分野】

本発明は、通信ユニット、情報通信システムおよび情報通信方法に関し、特に、データを暗号化して送信する通信ユニット、情報通信システムおよび情報通信方法に関する。

【0002】

【従来の技術】

従来、データ通信の際に、送信対象のデータの秘匿性を保持するために、データを送受信するのに先立って、ネットワーク接続されている他の通信ユニットとの間で、暗号化されたデータを復号化するための公開キーを交換しておき、データ送信側から暗号化したデータを送信し、データ受信側で送信されてきたデータを公開キーを用いて復号化していた。

【0003】

20

このような手法を採用するデータ転送方法について、特許文献1に記載がある。特許文献1には、送信部は、相手側の通信装置の受信部に公開キーを配送する。そして、通信電文を、受信側の通信装置の公開キーにより暗号化処理して送出する。当該通信電文を受信した受信部は、当該通信電文を、当該受信側の通信装置の秘密キーにより復号化処理して解読を行う、と記載されている。

【0004】

【特許文献1】

特開平09-093240号公報

【発明が解決しようとする課題】

しかし、従来の技術では、データ送信側の通信ユニットとデータ受信側の通信ユニットとを結ぶネットワークではデータの秘匿性が保持されるものの、データ送信側の通信ユニットあるいはデータ受信側の通信ユニットでは、ハッキング等により、データの秘匿性が保持されず、データが漏洩する場合があった。また、漏洩したデータが改ざんされることもあった。

【0005】

そこで、本発明は、データ送信側の通信ユニットあるいはデータ受信側の通信ユニットにおけるデータの漏洩、データの改ざんを防止することを課題とする。

【0006】

【課題を解決するための手段】

上記課題を解決するために、本発明は、データを送受信するのに先立って、ネットワーク接続されている他の通信ユニットとの間で、データを暗号化するための公開キーを交換するとともに、データの受信時には初回の当該データの受信前に前記他の通信ユニットに対して秘匿性が保持されるルートを通じて前記データに付加させるパスワードを送り、かつ当該他の通信ユニットに対して送信対象のデータに前記パスワードを付加してから自己の公開キーを用いて暗号化してなる暗号化データを作成するように促し、実際に当該他の通信ユニットから送信されてきた前記暗号化データを自己の公開キーに対応する秘密キーを用いて復号化を行い、データの送信時には当該送信前に前記他の通信ユニットから秘匿性が保持されるルートを通じて送信されたパスワードを付加した送信対象のデータを当該他の通信ユニットの公開キーを用いて暗号化することによって作成した暗号化データを前記他の通信ユニットに対して送信する通信ユニットであって、前記他の通信ユニットから送

50

(4)

JP 2005-20105 A 2005.1.20

信された暗号化データを記憶する第1の記憶部と、前記他の通信ユニットに送信する暗号化データを記憶する第2の記憶部と、前記他の通信ユニットから送信された暗号化データを前記第1の記憶部に書き込むとともに前記他の通信ユニットに送信する暗号化データを前記第2の記憶部から読み出す第1の情報処理装置と、前記第1の記憶部に記憶されている暗号化データを読み出して前記自己の秘密キーを用いて復号化する第2の情報処理装置と、前記第2の情報処理装置によって復号化されたデータに付加されていたパスワードとあらかじめ前記他の通信ユニットに送ったパスワードとを認証する認証手段と、前記認証手段によってパスワード相互の一致が確認されたときに前記第1の記憶部に記憶されている暗号化データを復号化したデータを取得するとともに前記他の通信ユニットへ送信する暗号化データを前記第2の記憶部に書き込む第3の情報処理装置とを備える。

10

【0007】

また、前記認証手段は、ディスプレイ、プリンタ、スピーカ、前記パスワードをパスするフィルタのいずれかである。

【0008】

さらに、本発明の情報通信システムは、上記通信ユニットを複数備え、当該通信ユニット相互をネットワークで接続してなる。

【0009】

さらにまた、本発明は、データを送受信するのに先立って、ネットワーク接続されている通信ユニット間で、データを暗号化するための公開キーを交換するとともに、初回の当該データの送受信前にデータ送信先の通信ユニットからデータ送信元の通信ユニットに対し  
て秘匿性が保持されるルートを通じて前記データに付加させるパスワードを送り、前記データ送信元の通信ユニットで、前記パスワードを付加した送信対象のデータを前記データ送信先の通信ユニットの公開キーを用いて暗号化することによって作成した暗号化データを、前記データ送信先の通信ユニットに対して送信するとともに、前記データ送信先の通信ユニットで、前記データ送信元の通信ユニットから送信されてきた暗号化データを自己の公開キーに対応する秘密キーを用いて復号化を行う情報通信方法であって、前記データ送信元の通信ユニットは、第1の情報処理装置によって、前記データ送信先の通信ユニットへ送信する暗号化データを第1の記憶部に書き込み、前記ネットワークに直接接続している第2の情報処理装置によって、前記第1の記憶部に記憶してある暗号化データを読み出し、前記データ送信先の通信ユニットは、前記ネットワークに直接接続している第3の情報処理装置によって、前記データ送信元の通信ユニットから送信されてきた暗号化データを第2の記憶部に書き込み、第4の情報処理装置によって、前記第2の記憶部に記憶してある暗号化データの復号化を行い、前記第4の情報処理装置によって復号化されたデータに付加されていたパスワードとあらかじめ送っているパスワードとが一致した場合に、第5の情報処理装置によって、前記第2の記憶部に記憶されている暗号化データを復号化したデータを取得する。

20

30

【0010】

【発明を実施するための形態】

以下、本発明を実施するための形態について、図面を参照して説明する。

【0011】

(実施形態1)

図1は、本発明の実施形態1の情報通信システムの模式的な構成を示すブロック図である。

40

【0012】

図1には、以下説明する通信ユニット100と通信ユニット200とが、インターネット、アナログ電話回線、ISDN電話回線、DSL、CATV、光ファイバ、ether Net、10BASE-T、100BASE-T、赤外線、無線などのネットワーク300を通じて接続されており、相互にデータ通信を行えるようにしている。

【0013】

また、情報処理装置130と情報処理装置140、150とは、互にデータの入出力を行

50

(5)

JP 2005-20105 A 2005.1.20

えるように、ローカルエリアネットワーク（以下、「LAN」と称する。）180あるいはイントラネットなどによって接続されている。

【0014】

通信ユニット100側と通信ユニット200側との間では、データを送受信するのに先立って、それぞれ、一対の公開キーと秘密キーとを作成する。公開キーはデータを暗号化する際に用い、秘密キーは暗号化されているデータを復号化する際に用いる。そして、相互に公開キーを交換してある。

【0015】

通信ユニット100、200は、ともに、データ送信元となる場合には、送信対象のデータと後述するパスワードとを、相手方の公開キーを用いて暗号化することによって作成した暗号化データを、データ送信先である通信ユニット200、100に対して送信する。一方、通信ユニット100、200は、ともに、データ送信先となる場合には、通信ユニット200、100で通信ユニット100、200から送信された暗号化データを受信して、自己の秘密キーを用いて復号化を行う。こうして、ネットワーク300上におけるデータの漏洩を防止している。

【0016】

さらに、本実施形態では、たとえば通信ユニット100から通信ユニット200に対してデータを送信する場合には、通信ユニット200から通信ユニット100宛てに、秘匿性が保持されるルートを通じて送信対象のデータに付加させるパスワードを送るようにしている。

【0017】

具体的には、初回のデータを送受信するのに先立って、パスワードをデータの受信側の通信ユニットからデータの送信側の通信ユニットに送っておくようにしている。秘匿性が保持されるルートには、たとえば記憶媒体を通じた郵送によるルート、ネットワーク300およびこれ以外の電話線等のネットワークによるルートがある。

【0018】

また、これに代えて、たとえば通信ユニット100は、通信ユニット200向けのパスワードを通信ユニット200の公開鍵で施錠し、通信ユニット200にメールすることでパスワードを通信ユニット200へ送るようにしてもよく、さらには通信ユニット100側でホームページを有している場合には、通信ユニット200の公開鍵で施錠したパスワードを、そのホームページに掲載するようしてもよい。<b>  
</b>

【0019】

通信ユニット100は、以下説明する情報処理装置110～130と、ハードディスク（以下、「HD」と称する。）160、170と、パスワードパスフィルタ190とを有している。

【0020】

情報処理装置110は、通信ユニット200から送信された暗号化データをHD170に書き込むとともに、通信ユニット200への送信対象の暗号化データをHD160から読み出すものである。

【0021】

情報処理装置120は、HD170に記憶されている暗号化データを読み出して、その暗号化データを自己の秘密キーで復号化し、復号化したデータおよびパスワードをパスワードパスフィルタ190へ出力するものである。

【0022】

情報処理装置130は、情報処理装置120によって読み出された暗号化データに付随するパスワードと予め通信ユニット200へ送っているパスワードとの認証を行い、暗号化データの送信元が通信ユニット100であるという確認をしたときに、HD170に記憶されているデータを読み出すとともに、通信ユニット200への送信対象の暗号化データをHD160に書き込むものである。

(6)

JP 2005-20105 A 2005.1.20

【0023】

HD160は、通信ユニット200宛てに送信する暗号化データを記憶するものである。

【0024】

HD170は、通信ユニット200から送信された暗号化データを記憶するものである。

【0025】

なお、HD160、170は、記憶媒体としての例示であり、DVD-RAM、半導体ディスク等のような外部記憶装置と称される記憶媒体を用いるようにしてもよい。

【0026】

パスワードパスフィルタ190は、パスワードの認証を情報処理装置130で行えるようにするために、パスワードだけを通し、他の属性のデータを通さないようするものである。パスワードパスフィルタ190は、情報処理装置120、130に設けられているたとえばプリンタポート、USBポートに接続されている。

【0027】

なお、パスワードパスフィルタ190に代えて、ディスプレイ、プリンタ、スピーカなどのように、通信ユニットのユーザに対してパスワードを可視、可聴等によって報知可能なものを備え、ユーザが目視等によってパスワードの認証を行うようにしてもよい。パスワードパスフィルタ190としてはたとえばキャラクタデータだけを透過するキャラクタパスフィルタを用いることができる。

【0028】

通信ユニット200は、それぞれ情報処理装置110～130に相当する情報処理装置210～230と、HD160、170に相当するHD260、270と、パスワードパスフィルタ190に相当するパスワードパスフィルタ290とを有している。

【0029】

図2は、図1に示す通信ユニット100の模式的な内部構成を示すブロック図である。なお、通信ユニット200も通信ユニット100と同様の構成としている。

【0030】

図2に示すように、情報処理装置130は、以下説明するCPU131と、メモリ132と、パスワード受取手段133と、パスワード更新手段134と、リセット命令手段135と、認証手段136、USBポート137と、第1ヘッド138と、第2ヘッド139とを備えている。

【0031】

CPU131は、HD170から読み出した暗号化データの復号化処理を含む、種々の演算を実行することにより情報処理装置130本体の動作の制御を司るものである。

【0032】

メモリ132は、主としてCPU131で実行するプログラムやデータを格納してあるものである。

【0033】

【0034】

パスワード受取手段133は、情報処理装置120側から出力される、通信ユニット200から送信された暗号化データに付随するパスワードを受け取るものである。

【0035】

パスワード更新手段134は、通信ユニット200に送信する暗号化データを、たとえば乱数等を用いて更新するものである。なお、パスワードの更新は、たとえば内部犯行、すなわち情報処理装置130本体を不正操作することなどによるパスワードの漏洩に対処するために、暗号化データの交換の度にあるいは定期的に行うようにしている。

【0036】

リセット命令手段135は、第2ヘッド139によって、通信ユニット200から送信された暗号化データ読み出した後に、情報処理装置120で読み出してある、通信ユニット200からの暗号化データと復号化後のデータおよびパスワードとをリセットする、あるいは情報処理装置120をリブートするように命令するものである。

(7)

JP 2005-20105 A 2005.1.20

## 【0037】

認証手段136は、あらかじめ通信ユニット200に送っているパスワードとパスワード受取手段133によって入力したパスワードとが一致しているか否かの認証を行うものである。

## 【0038】

USBポート137は、既述のように、パスワードパスフィルタ190と情報処理装置130本体とを接続するポートである。

## 【0039】

第1ヘッド138は、通信ユニット200に送信する暗号化データをHD160に書き込むことが可能なヘッドである。CPU131からの命令に応じて、暗号化データの書き込み位置にシークされ、通信ユニット200へ送信する暗号化データの書き込みが行われる。なお、第1ヘッド138は、ハード的に通信ユニット200に送信する暗号化データをHD160に書き込みする専用ヘッドとしてもよいし、汎用的なヘッドをソフト的に制御して通信ユニット200に送信する暗号化データをHD160に書き込む専用としてもよい。

## 【0040】

第2ヘッド139は、通信ユニット200から送信されHD170に記憶されている暗号化データを消去することが可能または読み出しすることが可能なヘッドである。認証手段136によってパスワード相互が一致していると判定されたことを条件として、CPU131からの命令に応じて、暗号化データの消去位置または読み出し位置にシークして、通信ユニット200から送信された暗号化データの消去または読み出しが行われる。なお、第2ヘッド139は、通信ユニット200から送信されHD170に記憶されている暗号化データを消去または読み出しする専用ヘッドとしてもよいし、汎用的なヘッドをソフト的に制御して通信ユニット200から送信されHD170に記憶されている暗号化データの消去専用または読み出し専用としてもよい。

## 【0041】

情報処理装置110は、以下説明するCPU111と、メモリ112と、第1ヘッド113と、第2ヘッド114とを備えている。

## 【0042】

CPU111は、種々の演算を実行することにより情報処理装置110本体の動作の制御を司るものである。

## 【0043】

メモリ112は、主としてCPU111で実行するプログラムやデータを格納してあるものである。

## 【0044】

第1ヘッド113は、HD160に記憶されている、通信ユニット200に送信する暗号化データを読み出しすることが可能なヘッドである。CPU111からの命令に応じて、暗号化データの読み出し位置にシークされ、通信ユニット200へ送信する暗号化データの読み出しが行われる。

## 【0045】

第2ヘッド114は、通信ユニット200から送信された暗号化データをHD170に書き込むことが可能なヘッドである。CPU111からの命令に応じて、第2ヘッド114をデータの書き込み位置にシークされ、通信ユニット200から送信された暗号化データの書き込みが行われる。

## 【0046】

なお、第1ヘッド113、第2ヘッド114は、それぞれ第1ヘッド138、第2ヘッド139と同様に、ハード的に実現してもよい、ソフト的に実現してもよい。

## 【0047】

情報処理装置120は、以下説明するCPU121と、メモリ122と、リセット手段123と、パスワード出力手段124と、プリンタポート128と、ヘッド129とを備え



(8)

JP 2005-20105 A 2005.1.20

ている。

【0048】

CPU121は、HD170から読み出した暗号化データの復号化処理を含む、種々の演算を実行することにより情報処理装置120本体の動作の制御を司るものである。

【0049】

メモリ122は、主としてCPU121で実行するプログラムやデータを格納してあるものである。

【0050】

リセット手段123は、リセット命令手段135からの命令に従って、HD170から読み出してある、通信ユニット200からの暗号化データと復号化後のデータおよびパスワードとをリセットする、あるいは情報処理装置120本体をリブートするものである。なお、リセット手段123とリセット命令手段135とに代えて、情報処理装置130で暗号化データを取得したことを検知する検知手段と検知手段による検知に応じて情報処理装置120側で自動的に情報処理装置120本体をリブート等する手段とを備えるようにしてもよい。

【0051】

パスワード出力手段124は、通信ユニット200から送信された暗号化データに付随するパスワードを出力するためのものである。

【0052】

プリンタポート128は、既述のように、パスワードパスフィルタ190と情報処理装置120本体とを接続するポートである。

【0053】

ヘッド129は、通信ユニット200から送信されHD170に記憶されている暗号化データを読み出し可能なヘッドである。CPU121からの命令に応じて、暗号化データの読み出し位置にシークされ、通信ユニット200から送信された暗号化データの読み出しが行われる。ヘッド129による動作は、第1ヘッド138、第2ヘッド139等と同様に、ハード的に実現してもよい、ソフト的に実現してもよい。

【0054】

なお、第1ヘッド113、ヘッド129は、それぞれ、数秒毎にHD160、170にアクセスして、暗号化データが書き込まれているか否かを判定し、暗号化データが書き込まれている場合には、それを読み出すようにしている。あるいは、たとえば第2ヘッド114、第1ヘッド138による暗号化データの書き込み完了をトリガとして光を出射する光出射器と、この光出射器から出射される光を受光可能な位置に光入射器を備えるようにして、光入射器で光を検知したことを条件として第1ヘッド113、ヘッド129によって暗号化データを読み出すようにしている。または、第2ヘッド114、第1ヘッド138による暗号化データの書き込み完了をトリガとしてフラグが書き換えられるステータスレジスタを設け、第1ヘッド113、ヘッド129側で、数秒毎にステータスレジスタにアクセスすることによって、暗号化データが書き込まれているか否かを判定し、暗号化データが書き込まれている場合には、それを読み出すようにしている。

【0055】

こうして、CPU111、131相互を接続することなく、HD160、170の暗号化データの書き込み完了後に、暗号化データを読み出し可能としている。

【0056】

図3は、図1、図2に示す情報通信システムの動作の説明図である。なお、ここでは、情報処理装置150から情報処理装置240に向けてデータを送信する場合を例に動作の説明を行う。太線で図示している接続線は、データの流れを示す。

【0057】

まず、既述のように、通信ユニット100、200間で相互の公開キーを交換するとともに、通信ユニット200から通信ユニット100宛にパスワードを送信しておく。

【0058】

(9)

JP 2005-20105 A 2005.1.20

この状態で、情報処理装置150は、送信対象のデータを情報処理装置130へLAN180を介して出力する。

【0059】

情報処理装置130は、情報処理装置150から出力された送信対象のデータに、通信ユニット200から得られたパスワードをCPU131等によって付加する。そして、これらを、通信ユニット200側の公開キーを用いて暗号化することによって暗号化データを作成する。作成した暗号化データは、CPU131、第1ヘッド138等を用いてHD160に書き込む。

【0060】

なお、2回目以降のデータの送受信の際には、上記パスワードを送信対象のデータに付加するか、パスワード更新手段134によって更新されたパスワードを送信対象のデータに付加することになる。

【0061】

ちなみに、情報処理装置140、150側に、通信ユニット200から送られたパスワードを出力しておくとともに、情報処理装置140、150側で通信ユニット200側の公開キーを記憶しておき、情報処理装置140、150側で暗号化データを作成可能とし、暗号化データを情報処理装置140、150から情報処理装置130へ出力するようにしてもよい。

【0062】

ここで、本実施形態では、第1ヘッド113は、HD160に定期的にアクセスして、暗号化データが書き込まれているか否かを判定しており、ここでは暗号化データをHD160に書き込みを行ったので、この暗号化データが第1ヘッド113によって読み出される。そして、読み出された暗号化データは、図示しない送信手段およびネットワーク300を通じて、通信ユニット100側から通信ユニット200側へと送信される。

【0063】

通信ユニット200側では、情報処理装置210によって、通信ユニット100側からの暗号化データが受信され、HD270に書き込まれる。

【0064】

つづいて、情報処理装置220は、HD270への暗号化データの書き込み完了を検知すると、この暗号化データを読み出す。読み出した暗号化データは、自己の秘密キーを用いて復号化する。こうして、情報処理装置150から送信されたデータおよびパスワードを取得する。ひきつづき、情報処理装置220は、取得したデータおよびパスワードを、プリンタポート128等を介してパスワードパスフィルタ290へ出力する。

【0065】

パスワードパスフィルタ290は、情報処理装置220から出力されたデータおよびパスワードを入力すると、キャラクタデータ以外の属性のデータを除去することによって、パスワードを情報処理装置230へ出力する。

【0066】

情報処理装置230は、パスワードパスフィルタ290から出力されたパスワードを入力すると、このパスワードとあらかじめ通信ユニット100へ送ってあるパスワードとを認証手段136によって認証する。

【0067】

認証の結果、パスワード相互が一致していない場合には、HD270に書き込まれている暗号化データは所要のものでなく、たとえばウィルスを含んでいる可能性もあるので、情報処理装置230は、HD270に記憶されている暗号化データをデリートするとともに、情報処理装置220に対してHD270から読み出した暗号化データ等のデリート命令をする。なお、図示しない報知手段によって、暗号化データが所要のものでない旨を、通信ユニット200のユーザに報知するようにしてもよい。

【0068】

一方、パスワード相互が一致している場合には、HD270に書き込まれている暗号化デ

(10)

JP 2005-20105 A 2005.1.20

ータは所要のものであるので、情報処理装置230は、この暗号化データをHD270から読み出して、自己の秘密キーによって復号化する。

【0069】

なお、情報処理装置220ですでに暗号化データが復号化されていることとHD270で使用するチャネル数を3チャネルから2チャネルに減らせるということとを考慮して、パスワードパスフィルタ290を含むルートと並列に情報処理装置220、230間を直接接続可能な別ルートを設けておき、情報処理装置230は、パスワード相互が一致している場合にだけ物理的に別ルートを開通させ、情報処理装置220で復号化されたデータを別ルートを介して入力するようにしてもよい。こうすると、情報処理装置230にネットワーク300の外部からの進入を防止しつつ、情報処理装置230で通信ユニット100側からのデータを取得することができる。

【0070】

その後、情報処理装置230は、LAN280を通じて情報処理装置240宛に復号化済みのデータを出力する。それから、情報処理装置220に対して暗号化データ等をリセットするように命令する。さらに、パスワードを更新することによって、次のデータ通信の際に使用するパスワードを用意して、更新したパスワードと更新前のパスワードとを情報処理装置130へ送信しておく。

【0071】

情報処理装置220は、情報処理装置230からの命令に従って、HD270から読み出した暗号化データ等をリセットして、次回、通信ユニット100から送信されてくる暗号化データの入力を可能とする。

【0072】

また、情報処理装置130は、更新前後のパスワードを受信すると、更新前のパスワードを更新後のパスワードに書き換え、次回からのデータの送信時には更新後のパスワードを付加するようにするとともに、次回からのデータの受信時の認証を行えるようにする。

【0073】

以上説明したように、本実施形態では、通信ユニット100、200間で種々のデータの送受信をする際に、外部から情報処理装置130、230に対する進入を防止している。

【0074】

(実施形態2)

本発明の実施形態2として、図1に示す情報通信システムを、会員制ホームページの維持・管理に用いる場合を例に説明する。この会員制ホームページには、ホームページの管理者側のEメールアドレスが掲載されており、会員と管理者側との間でEメールの送受信を行えるようにしている。

【0075】

図1に示す情報通信システムを、たとえば会員制ホームページの維持・管理に用いる場合には、会員制ホームページのシステム管理者側と会員との間で公開キーの交換をし、会員制ホームページのシステム管理者から会員に対してパスワードを発送等しておく。

【0076】

そして、会員制ホームページのシステム管理者側は、会員制ホームページに掲載する情報等を会員が閲覧可能とするために、その情報等を暗号化してから第1ヘッド138によりHD160へ書き込む。

【0077】

このホームページを閲覧しようとする会員は、ネットワーク300を介して通信ユニット100にアクセスする。これにより、情報処理装置110ではHD160に書き込まれている情報等を第1ヘッド113で読み出して、会員側へ送信する。会員は、自己の秘密キーを用いて、通信ユニット100から送信されてきた情報等を復号化することによって、その情報等を閲覧可能とする。

【0078】

この場合、第1ヘッド113は、読み出し専用ヘッドであるため、HD160に書き込ま

(11)

JP 2005-20105 A 2005.1.20

れている情報等が、会員を含む第三者、すなわち外部から改ざんされることはない。

【0079】

また、会員制ホームページに掲載している情報処理装置110に付随するEメールアドレス宛てに、会員からEメールを送信しようとする場合には、通信ユニット100側から発送されているパスワードを付加したEメールの情報を通信ユニット100の公開キーで暗号化して、ネットワーク300を経由して通信ユニット100へ送信する。

【0080】

この後の処理は、実施形態1で説明したとおり、送信されてきたEメールのHD170への書き込みを情報処理装置110で行い、HD170に書き込みされているEメールの復号化を情報処理装置120で行い、復号化されたパスワードと発送しているパスワードとの認証を情報処理装置130で行い、認証確認ができたことを条件としてHD170に書き込みされているEメールの復号化をたとえば情報処理装置130で行う。このため、Eメールの内容は外部に曝されることがないし、改ざんされることもない。

【0081】

また、本実施形態では、会員制ホームページの維持・管理に用いる場合を例に説明したが、たとえば公共工事の入札をオンラインで行う場合にも適用できる。この場合にも、入札状況が外部に漏れることがないし、改ざんされることもない。

【0082】

(実施形態3)

図4は、本発明の実施形態3の情報通信システムの模式的な構成を示すブロック図である。なお、図4において、図2に示す部分と同様の部分には同一符号を付している。

【0083】

図4に示すように、本実施形態では、図1等を示すHD160、170に代えてHD200を備えるとともに、第1ヘッド138および第2ヘッド139に代えてヘッド210を備え、第1ヘッド113および第2ヘッド114に代えてヘッド220を備えている。

【0084】

HD200は、HD160に相当する第1領域201と、HD170に相当する第2領域202とが形成されている。

【0085】

ヘッド210は、第1領域201に情報の書き込みが可能であり、かつ第2領域202から情報の読み出しが可能なヘッドである。

【0086】

ヘッド220は、第1領域201から情報の読み出しが可能であり、かつ第2領域202に情報の書き込みが可能なヘッドである。

【0087】

ヘッド129は、第2領域202から情報の読み出しが可能なヘッドである。

【0088】

なお、ヘッド210、220、129は、その専用機能をハード的に実現してもよいし、ソフト的に実現してもよい。

【0089】

本実施形態では、HD200とヘッド210、220とを備え、情報処理装置110、130でヘッド210、220に対して時間多重制御を行うことで、既述の効果を維持しつつ、部品数を減らすことによる情報通信システムの小型化・低廉化を実現している。

【0090】

(実施形態4)

本発明の実施形態4では、実施形態3で説明したHD200に第1領域201と第2領域202とを形成することなく、実施形態1の情報通信システムと同様の効果を奏する情報通信システムについて説明する。

【0091】

本実施形態の情報通信システムでは、HD200に記憶されている全てのファイルに、各

(12)

JP 2005-20105 A 2005.1.20

ヘッド210、220、129で扱えるファイルを特定するためのフラグを、各ヘッド210、220、129がHD200にファイルを書き込む際に、割り当てるようにしている。

【0092】

これらのフラグとしては、たとえばフラグA～Cを用意しておき、下記のように割り当てられている。なお、用意するフラグの数は3つに限定されず、各ヘッド210、220、129で扱えるファイルの特定要件を細分化して、4つ以上としてもよい。

【0093】

上記のように、ヘッド220は、フラグAが割り当てられたファイルだけを読み出し可能である。なお、書き込みの際には、ファイルにフラグBを割り当てる。

10

【0094】

ヘッド210は、いずれのフラグが割り当てられたファイルであっても読み出し可能である。なお、書き込みの際には、ファイルにフラグA～Cのいずれであっても割り当て可能である。

【0095】

さらに、ヘッド210は、既存のファイルに割り当てられているフラグの変更を行うことも可能であり、情報処理装置110はたとえばフラグBを割り当ててから書き込みしたファイルを読み出して、再度HD200に書き込みする際には、フラグCを割り当ててから、HD200に書き込むことができる。

【0096】

ヘッド129は、フラグCが割り当てられたファイルだけを読み出し可能である。

20

【0097】

なお、ヘッド210、220、129は、その専用機能をハード的に実現してもよいし、ソフト的に実現してもよい。

【0098】

本実施形態では、部品数の削減による情報通信システムの小型化・低廉化の実現のみならず、HD200という汎用的なHDを備えることで、さらなる情報通信システムの低廉化を実現している。

【0099】

以上、本発明の各実施形態では、複数の情報処理装置110～130等を含む情報通信システム100、200を例に説明したが、情報通信システム100、200は、たとえば半導体化して作り上げるようにしてもよい。

30

【0100】

また、HD160、HD170、HD260、HD270、HD200、とそれらの持つヘッドは既存の1ヘッドハードディスクに、複数の入出力チャネルを持つ例えば時間多重制御基盤を付加する事によってその専用機能を実現してもよい。

【0101】

【発明の効果】

以上説明したように、本発明によると、データ送信側の通信ユニットあるいはデータ受信側の通信ユニットに備える記憶部に、ネットワークを通じて送信されてきた情報が書き込まれた後には、その情報をネットワークに接続されている外部の通信ユニットから読み出しを行えないようにしているので、データの漏洩、データの改ざんを防止することができる。

40

【図面の簡単な説明】

【図1】 本発明の実施形態1の情報通信システムの模式的な構成を示すブロック図である。

【図2】 図1に示す通信ユニット100の模式的な内部構成を示すブロック図である。

【図3】 図1、図2に示す情報通信システムの動作の説明図である。

【図4】 本発明の実施形態3の情報通信システムの模式的な構成を示すブロック図である。

50

(13)

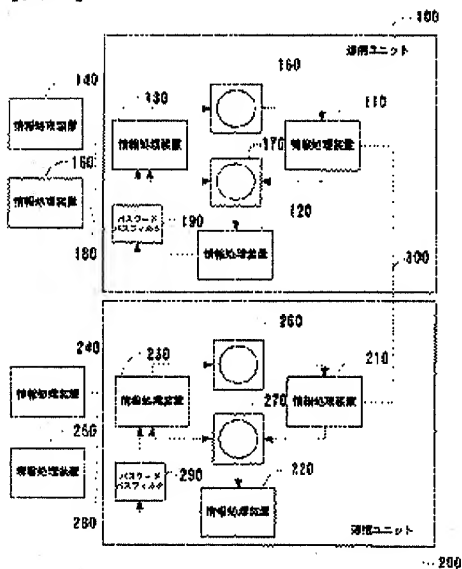
JP 2005-20105 A 2005.1.20

## 【符号の説明】

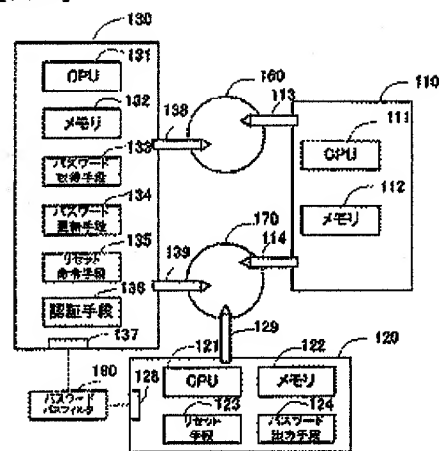
110～150、210～250 情報処理装置  
 160、170、260、270 HD  
 190、290 パスワードパスフィルタ  
 111、121、131 CPU  
 112、122、132 メモリ  
 123 リセット手段  
 124 パスワード出力手段  
 128 プリントポート  
 133 パスワード受取手段  
 134 パスワード更新手段  
 135 リセット命令手段  
 113、138 第1ヘッド  
 114、139 第2ヘッド  
 136 認証手段  
 137 USBポート

10

【図1】



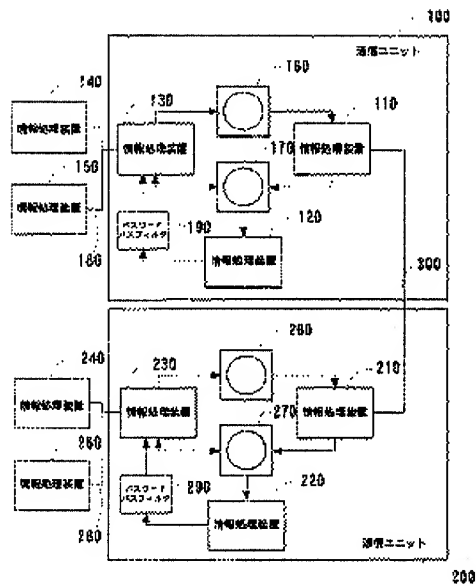
【図2】



(14)

JP 2005-20105 A 2005.1.20

【図 3】



【図 4】

